AMENDMENTS TO THE DRAWINGS

The attached sheet(s) of drawings include changes to FIG. 10.

Specifically, FIG. 10 has been amended to conform to the description in the specification at page 17, line 26, to page 18, line 6, which states: "A ciphertext C'_4030 is divided into 64-bit blocks, and the resultant ciphertext blocks are specified as C'_1_4035, C'_2_4036, ..., C'_N_4037, C'_{N+1}_4038, and C'_{N+2}_4039. Next, $NH_R(S)$ is computed, selecting R and S as the inputs. Here, R results from connecting R_2_4021, R_3_4022, ..., and R_{N+1}_4028 in this sequence, and S results from connecting C'_1_4035, C'_2_4036, ..., and C'_N_4037 in this sequence. If $NH_R(S) = C'_{N+1}$_4038 $\| C'_{N+2}$_4039, the processing proceeds to the next step."

REMARKS

In response to the pending Office Action, claims 1, 4, 5, 10, and 12 are amended. Claims 2, 3, 6-9, 11, and 13-23 are cancelled without prejudice. Claims 24-29 are new. No new matter is added. Claims 1, 10, 25, and 28 are the only independent claims.

Claims 1-23 are rejected under 35 U.S.C. § 102(b) as being anticipated by Gligor (U.S. Patent Application Publication 2002/0048364). This rejection is traversed. Applicants submit that this rejection is moot with respect to cancelled claims 2, 3, 6-9, 11, and 13-23.

Independent claim 1 recites, in part, "an **encryption operation unit for generating random-number blocks R_i ($1 \le i \le N+1$) from a secret key, wherein the number of the random-number blocks R_i is greater than that of the plaintext blocks P_i**, and performing an encryption operation for ciphertext blocks C_i ($1 \le i \le N$) by using the plaintext blocks P_i ($1 \le i \le N$) and the random-number blocks R_i ($1 \le i \le N$), wherein the number N of the random number blocks is the same as that of the ciphertext blocks."

As is well known, anticipation under 35 U.S.C. § 102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed Cir. 1987). The elements must be arranged as required by the claim. *In re Bond*, 910 F. 2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). At a minimum, the cited prior art does not disclose (expressly or inherently) the above recited encryption operation.

The Office Action, at pages 2 and 3, asserts the Gligor discloses the claimed encryption operation at paragraph 163. However, Gligor, at paragraph [0163], states merely:

> [0163] The application of the combination operation 84 to the plurality of hidden ciphertext blocks 87 and the unpredictable elements 83 of the sequence results in a plurality of ciphertext blocks y_i 24. Ciphertext block y_0 25 and the plurality of ciphertext blocks y_j 24 form the ciphertext string y 26 that has n+2 blocks and is

the output data of the encryption mode 51. For the example presented in FIG. 1, the ciphertext string 26 is $y= y_0 y_1 y_2 y_3 y_4 y_5$; i.e., has n+2=6 blocks.

Thus, Gilgor does not teach or suggest "**generating random-number blocks R_i ($1 \leq i \leq N+1$) from a secret key, wherein the number of the random-number blocks R_i is greater than that of the plaintext blocks P_i,**" as recited by claim 1.

Thus, at a minimum, the Gligor fails to teach or suggest the forgoing generating limitation, and therefore claims 1 is novel over the cited art. Withdrawal of the art rejection is requested, and should render claim 1 allowable over the cited art.

Applicants submit that independent claims 10, 25, and 28 are allowable for reasons similar to independent claim 1.

Under Federal Circuit guidelines, a dependent claim is allowable if the independent claim upon which it depends is allowable because all the limitations of the independent claim are contained in the dependent claims, *Hartness International Inc. v. Simplimatic Engineering Co.*, 819 F.2d at 1100, 1108 (Fed. Cir. 1987).

Thus, as independent claim 1, 10, 25, and 28 are allowable for the reasons set forth above, it is respectfully submitted that dependent claims 4, 5, 12, 24, 26, 27, and 29 are allowable for at least the same reasons as their respective base claims.

Accordingly, it is urged that the application, as now amended, is in condition for allowance, an indication of which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, Examiner is requested to call the undersigned attorney at the telephone number shown below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Ed Garcia-Otero

Eduardo Garcia-Otero
Registration No. 56,609

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 KEG/EG:dp
Facsimile: 202.756.8087
Date: January 28, 2008

Please recognize our Customer No. 20277 as our correspondence address.

WDC99 1518896-2.062807.0167